

core

github.com/home-assistant/core

Scanned 07 October 2026 at 05:08 · Report generated 29 October 2026 · Python · 91,283 stars

OVERALL ASSESSMENT

High

Combined score 86 · 71 findings after filtering

Summary

The repository has a very low vulnerability score of 0.0, which means there are no obvious code errors that could be easily exploited by attackers. However, the high malicious-pattern score of 86.0 indicates that the code contains many signs of intentional bad behavior rather than just standard mistakes. The most serious issues involve potential credential harvesting and download-and-execute attacks, as well as suspicious dependencies like typosquatting names for popular libraries. These findings suggest the code may be actively trying to steal secrets or run malicious scripts, which is a much more dangerous situation than simple insecure coding patterns.

Written by a language model running locally on the scanning machine, from the findings in this report. The risk levels above and below were decided by the scoring model, not by this summary.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

Safe (0)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

High (86)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
yara	Signatures of malicious behaviour in source files	11	0	37	48
guarddog	Malicious package and install-time behaviour	3	9	0	12

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
dep_checker	Vulnerable, unpinned or typosquatted dependencies	2	1	8	11

15 of 71 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. "Seen" is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	guarddog	Detects keylogging and input capture patterns [threat-runtime-keylogging]	3	/homeassistant/components/keyboard_remote/__init__.py:10
HIGH	dep_checker	Typosquatting: 'httpx2' is suspiciously similar to 'httpx'	2	pyproject.toml
HIGH	yara	YARA rule matched: detect_credential_harvester — References credential/secret material by name AND a deliberate outbound-send API in the same file - narrower than 'reads any env var', which large legitimate codebases do constantly regardless of intent. Still not proof the two are connected (YARA c	3	/homeassistant/components/pushsafer/notify.py
HIGH	yara	YARA rule matched: detect_base64_exec — Encoded payload decoded and then executed	2	/homeassistant/helpers/template/extensions/base64.py
HIGH	yara	YARA rule matched: detect_download_and_execute — Downloads a remote resource AND executes it - the actually dangerous combination, not just downloading alone	6	/CLAUDE.md

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
MEDIUM	guarddog	Detects extensive system/network enumeration activities [threat-runtime-enumeration]	3	/homeassistant/components/nmap_tracker/____init__.py:12
MEDIUM	guarddog	Detects unicode homoglyphs and uncommon characters used for obfuscation [threat-runtime-obfuscation-unicode]	1	/homeassistant/const.py:561
MEDIUM	guarddog	Detects URLs to suspicious domains often used for exfiltration or C2 [threat-network-exfiltration]	3	/homeassistant/components/marketplace/system_health.py:46
MEDIUM	guarddog	Detects URLs to URL shorteners, file sharing, and suspicious services [threat-network-outbound-shady-links]	2	/homeassistant/components/route53/____init__.py:98
MEDIUM	dep_checker	Unpinned dependency: '-c homeassistant/package_constraints.txt' has no version lock — supply chain risk	1	requirements.txt:3
LOW	dep_checker	Loose version constraint: 'certifi>=2021.5.30' — attacker could push malicious update	2	pyproject.toml
LOW	dep_checker	Loose version constraint: 'packaging>=23.1' — attacker could push malicious update	2	requirements.txt:39
LOW	dep_checker	Loose version constraint: 'typing-extensions>=4.16.0,<5.0' — attacker could push malicious update	2	requirements.txt:58
LOW	dep_checker	Loose version constraint: 'urllib3>=2.0' — attacker could push malicious update	2	requirements.txt:60

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
LOW	yara	YARA rule matched: detect_downloader — Downloads a remote resource - common and low-signal alone; see detect_download_and_execute for the composite version	37	/homeassistant/components/route53/__init__.py

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 07 October 2026.